(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 41 776 A1**

(51) Int. Cl.[6]:
H 04 L 12/22
G 07 F 19/00
G 06 F 17/50

(21) Aktenzeichen: 196 41 776.7
(22) Anmeldetag: 4. 9. 96
(43) Offenlegungstag: 13. 3. 97

DE 196 41 776 A1

Mit Einverständnis des Anmelders offengelegte Anmeldung gemäß § 31 Abs. 2 Ziffer 1 PatG

(71) Anmelder:
TeleCash Kommunikations-Service GmbH, 70174 Stuttgart, DE

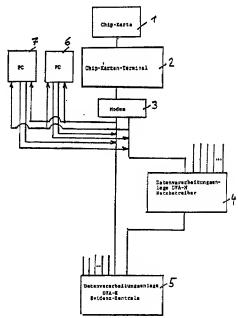
(74) Vertreter:
Blutke, K., Dipl.-Ing., Pat.-Anw., 71032 Böblingen

(72) Erfinder:
Matzke, Dietmar G., 61389 Schmitten, DE; Habel, Klaus, 65599 Dornburg, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Computerprogrammgesteuertes Verfahren zum gesicherten Aufbau einer Wähl-Leitungsverbindung und zur gesicherten Datenübertragung zwischen einem Chipkarten-Terminal und einer zentralen Datenverarbeitungsanlage

(57) Computerprogrammgesteuertes Verfahren zum gesicherten Aufbau einer Wähl-Leitungsverbindung und zur gesicherten Datenübertragung zwischen einem Chipkarten-Terminal (2) und einer zentralen Datenverarbeitungsanlage (3, 4) unter Ausschluß unbefugten Zugriffes auf die Leitungsverbindung und/oder die Daten.
Dieses Verfahren schließt eine gegenseitige Authentisierung der Datenverarbeitungsanlage und des Terminals mittels gegenseitig übertragener unverschlüsselter und verschlüsselter Zufallwerte, eine Überprüfung und ggf. Vergabe eines Terminal-Identifikations-Codes, Maßnahmen zur Verhinderung von Doppel-Abrechnungen und eine Löschung der im Terminal (2) zwischengespeicherten Bezahl-Daten etc. erst nach einer Akzeptanz-Prüfung ein.



DE 196 41 776 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 01. 97 802 071/614

BHPA00005700

Beschreibung

Die Erfindung betrifft ein computerprogrammgesteuertes Verfahren zum gesicherten Aufbau einer Wählleitungsverbindung und zur gesicherten Datenübertragung zwischen einem Chipkarten-Terminal und einer zentralen Datenverarbeitungsanlage unter Ausschluß unbefugten Zugriffes auf diese Leitungsverbindung und/oder die Daten.

Im Rahmen bargeldlosen Geldverkehrs werden auch sogenannte Chipkarten für den Einkauf von Waren o.ä. verwendet; aus dem Chip können gedachte Geldbeträge "entnommen" werden, bis sich der Vorrat an gedachtem Geld im Chip erschöpft hat.

Im Chip einer solchen Chipkarte ist in einem elektronischen Speicher u. a. ein einem Geldbetrag darstellender Wert (als Zahl) gespeichert. Bei einem Kaufvorgang wird dieser Wert um den jeweiligen Kaufpreis der Ware verringert, ein Vorgang der der Verwendung allgemein bekannter Telefonkarten ähnelt. Kaufvorgänge mit der Chipkarte können solange fortgesetzt werden, bis der gedachte Geldwert im Chip auf Null reduziert ist.

Für den Umgang mit der Chipkarte ist ein Gerät erforderlich, mit dessen Hilfe die im Chip gespeicherten Werte gelesen und ggfls. auch verändert werden können. Bei Telefonkarten verbirgt sich dieses Gerät hinter dem Apparate-Einsteckschlitz für die Telefonkarte. Für Chipkarten zum Einkauf von Waren o. ä. sind sogenannte Chipkarten-Terminals vorgesehen, die bei Händlern, in Dienstleistungsbetrieben etc. (bei Terminalbesitzern) aufgestellt sind. Für den Bezahlvorgang ist die Chipkarte in eine dafür vorgesehene Lese/Schreibstation des Terminals zu stecken. Das Terminal liest den in der Chipkarte enthaltenen Geldwert und verringert diesen um den Kauf(Bezahl)betrag. Der Kaufbetrag kann z. B. über eine Tastatur in das Terminal eingegeben worden sein. Es ist jedoch auch denkbar, daß die Eingabe des Kaufpreises in das Terminal auf andere Weise geschieht, z. B. über sogenannte Scanner, wie sie heute an fast allen Kaufhauskassen zur schnellen Erfassung der Preise verwendet werden.

Nach dem "Abbuchen" des Kaufpreises von dem im Chip gespeicherten Geldwert, der Verringerung dieses Wertes um den Kaufpreis, erhebt sich die Frage, wie nun z. B. der Händler, über dessen Terminal gekauft wurde, zu seinem Geld kommt, und dies bei einer Vielzahl von Terminals, die bei einer Vielzahl von Händlern aufgestellt sind. Alle diese Terminals sind über Telefonleitungen o.ä. mit einer zentralen Datenverarbeitungsanlage verbunden. Die an den Terminals bei Kaufvorgängen von den Chipkarten abgebuchten Bezahlbeträge werden pro Terminal zusammen mit anderen terminal-, chipkarten- und terminalbesitzerspezifischen Daten an die zentrale Datenverarbeitungsanlage übertragen. Im Rahmen der Übertragung und nach Empfang der übertragenen Daten durch die Datenverarbeitungsanlage finden verschiedene Prüfungen statt, bevor die Datenverarbeitungsanlage veranlaßt, daß dem betroffenen Terminalbesitzer (Händler) der über sein Terminal getätigte Umsatz auf seinem Bankkonto gutgeschrieben werden kann.

Die durchzuführenden Prüfungen sind unerläßlich, soll der Zugriff von Unbefugten auf die Übertragungsleitungen oder die zu übertragenden Daten verhindert werden. Die Prüfungen dienen weiterhin der Verhinderung von Fehlbuchungen und Datenverlusten- der Händler, der Terminalbesitzer, der auf sein Geld wartet, soll dieses auch sicher bekommen, hier in Form einer elektronischen Habenbuchung auf seinem Computer-Bankkonto.

Fig. 1 zeigt ein vereinfachtes Blockschaltbild mit einem Chipkarten-Terminal 2 und zentralen Datenverarbeitungsanlagen 4, 5 für einen bargeldlosen Geldverkehr mit einer Chipkarte. Der Aufbau der Leitungsverbindungen, die Datenübertragung und verschiedene computerprogrammgesteuerte Prüfungen und Maßnahmen können auf unterschiedliche Art, nach unterschiedlichen Verfahren erfolgen.

Ein bekanntes vorgeschlagene Verfahren steht im Zusammenhang mit dem sogenannten Z-Modem, einem Software-Übertragungsverfahren für eine Datei, die aus logisch zusammengefaßten Datensätzen besteht. Danach überträgt unter Beachtung vordefinierter Kriterien ein Sender eine Datei an einen Empfänger. Die Datei ist durch einen Dateinamen und ihre Länge definiert, sie wird in eine Vielzahl sogenannter Pakete aufgegliedert.

Die Datensätze sind verdichtet und mit Prüfziffern versehen.

Der Empfang von Paketen und der gesamten Datei wird vom Empfänger in Prüfintervallen an den Sender durch eine sogenannte Quittier-Information bestätigt. Die Anzahl der Pakete, die eine Quittierung nach sich zieht, kann je nach Anforderung dynamisch variabel sein.

Bei dem bekannten vorgeschlagenen Verfahren werden zuvor erwähnte Chipkarten verwendet.

Beim "Aufladen" der Chipkarten wird in diesen u. a.

1. eine Chip-Kennummer und
2. ein Ausgangs-Wertbetrag, z. B. DM 400.— eingeschrieben (elektronisch gespeichert).

Die Chip-Kennummer und der Wertbetrag können von einem Chipkarten-Terminal, in welche die Chipkarte für einen Kauf(Bezahl)vorgang eingeführt wird, gelesen werden. Der Kaufbetrag wird in das Chipkarten-Terminal über eine Tastatur eingegeben und automatisch von dem im Chip gespeicherten Wertbetrag abgezogen. Die verbleibende Differenz wird automatisch durch das Chip-Karten-Terminal im Chip anstelle des vorhergehenden Wertbetrages gespeichert.

Erfolgte z. B. ein Kauf für DM 10.—, so sind anstelle des ursprünglichen Wertbetrages von DM 400.— jetzt nur noch DM 390.— im Chip vermerkt; es kann also noch mehrfach eingekauft werden, bis auch dieser Betrag verbraucht ist.

Die Chipkarte gestattet somit ein bargeldloses Einkaufen.

Die Frage, wie nun der Händler zu seinem Geld kommt, wurde bereits vorstehend andeutungsweise beantwortet von den Chipkarten beim Einkauf auf einem Terminal abgebuchte Kauf(Bezahl)beträge werden zusammen mit anderen Daten, so auch der Händler-Bankverbindung elektronisch an eine zentrale Datenverarbeitungsanlage 5 weitergeleitet, an die die Terminals aller Händler durch Telefonanwahl angeschlossen sind.

Nach einigen Prüfungen der übermittelten Daten bewirkt diese Datenverarbeitungsanlage, daß jeder Händler einen entsprechenden Betrag für die bei ihm getätigten Einkäufe auf seinem Bankkonto gutgeschrieben bekommt. Allgemein hat sich für diese Art des bargeldlosen Einkaufes der Begriff "electronic cash" eingebürgert.

Beim Aufladen des Chips mit Kennummer und Wertbetrag wird zugleich in der zuvor erwähnten zentralen Datenverarbeitungsanlage 5, der sogenannten Evidenz-

BHPA00005701

Zentrale eine Schatten-Konto-Datei angelegt, in der unter dem Ordnungsbegriff der Kennummer des Chips auch der Wertbetrag der Chipkarte gespeichert ist. Gehen in der Evidenz-Zentrale Informationen ein, für welche Chipkarten welche Kaufbeträge abgebucht wurden, so wird dies aus Gründen der Sicherheit auch in der Schatten-Konto-Datei nachvollzogen. Die Abbuchung vom Schattenkonto bewirkt für den betroffenen Händler, von dessen Terminal der Chipkarten-Umsatz gemeldet wurde, daß auf seinem Computer-Bankkonto ein entsprechender Betrag gutgeschrieben wird.

Eine solche Buchung auf dem Bankkonto des Händlers erfolgt selbstverständlich nicht in der Datenverarbeitungsanlage DVA-E der Evidenz-Zentrale selbst. Die DVA-E ist mit den Computern angeschlossener Banken verbunden, in denen die Händler-Konten geführt werden. Die DVA-E überträgt an den entsprechenden Bank-Computer die Information, einem durch Namen und Bankverbindung ausgewiesenen Händler einen bestimmten Betrag gutzuschreiben.

Das verwendete Chipkarten-Terminal enthält eine elektronisch auslesbare Händlerkarte (Händler ist eine gängige Bezeichnung für einen Terminal-Besitzer, der nicht immer ein Händler sein muß, denn Dienstleistungsbetriebe u. a.m. pflegen neben Händlern ebenfalls einen bargeldlosen Geldverkehr), aus der neben der Händleridentifikation auch die Bankverbindung des Händlers ausgelesen und zusammen mit den Chipkarten-Buchungsdaten an die Evidenz-Zentrale übermittelt werden können.

Der Übermittlung der Daten geht eine telefonische Anwahl der Evidenz-Zentrale voraus, die Übertragung der Informationen erfolgt über ein herkömmliches Modem 3 und Telefonleitungen.

Neben der direkten Anwahl der Evidenz-Zentrale können die Informationen vorzugsweise zunächst an die Datenverarbeitungsanlage DVA-N 4 eines sogenannten Netzbetreibers geleitet werden. Dort erfolgt eine Verdichtung und Aufbereitung der empfangenen Daten. Unter spezifischer Kenntnis einer äußerst effizienten Zugangstechnik zur Evidenz-Zentrale werden die vom Netzbetreiber 4 "vorbehandelten" Daten an die Evidenz-Zentrale 5 weitergeleitet. Die Zwischenschaltung des Netzbetreibers 4 entlastet die Datenverarbeitungsanlage 5 der Evidenz-Zentrale so enorm, daß aus Wirtschaftlichkeitsgründen davon auszugehen ist, daß zu ca. 90% von dieser Zwischenschaltung des Netzbetreibers Gebrauch gemacht werden wird.

Das zuvor erwähnte bekannte Verfahren ist jedoch mit einer Reihe signifikanter Nachteile behaftet:

a) Nach dem Z-Modem-Übertragungsprotokoll erfolgt eine protokollbasierte (nicht logische) Quittierung des Empfanges von Informationen durch die Evidenz-Zentrale 5 an das sendende Terminal 2. Auf Grund dieser Quittierung werden die bis zu diesem Zeitpunkt im Terminal zwischengespeicherten Buchungsdaten, welche an die Evidenz-Zentrale 5 oder den Netzbetreiber 4 gesendet wurden, gelöscht. Dabei wird nicht berücksichtigt, ob die übertragenen Buchungsdaten – durch Hacker bewirkt – möglicherweise eine Gutschrift auf ein fremdes "Hacker"-Konto auslösen würden. Nach Löschung der zwischengespeicherten Buchungsdaten im Terminal, ausgelöst durch die Quittierung seitens der Evidenz-Zentrale, erhält bei einer Fremdkonto-Gutschrift der berechtigte Händler kein Geld, eine begründete Reklamation ist nicht möglich, da die zwischengespeicherten Daten gelöscht wurden und es in der Regel keinen Terminal-Ausdruck gibt.

b) Desweiteren ist es durch die manuelle telefonische Anwahl der DVA-N 4 des Netzbetreibers oder der DVA-E 5 der Evidenz-Zentrale für eine nachfolgende Datenübertragung möglich, versehentlich andere im Netz betriebene fremde PC's 6, 7 (oft als electronic mail boxes bezeichnet) anzuwählen, die nach dem Z-Modem-Übertragungsverfahren den Empfang der an sie gelangten Informationen dem Chipkarten-Terminal bestätigen. Dies löst wie zuvor in einem anderen Zusammenhang bemerkt, die Löschung der im Terminal zwischengespeicherten Buchungsdaten aus, abgehen davon, daß die vom fremden PC empfangenen Daten nicht an die Evidenz-Zentrale bzw. den Netzbetreiber weitergeleitet werden. Im schlimmsten Falle eines erfolgreichern kriminellen Hackers können die auf seinem PC empfangenen Daten manipuliert und weitergeleitet werden, um eine Gutschrift auf einem "Hacker"-Konto zu bewirken.

c) Ebenso ist es denkbar, daß ein Hacker Buchungsdaten einer Chipkarte simuliert und zur Auslösung einer Bankgutschrift auf ein "Hacker"-Konto benutzt.

d) Als Nachteil kann es sich auswirken, daß bei der Vergabe von Datei-Namen die gleiche Bezeichnung mehrfach vergeben und benutzt wird. Eine in der Evidenz-Zentrale unter einem bestimmten Dateinamen gespeicherte Datei wird beim Eintreffen einer gleichbenannten Datei von dieser überschrieben, um Mehrfach-Gutschriften bei Mehrfachsendungen derselben Datei zu vermeiden. Diese Regelung hat jedoch den Nachteil, daß unterschiedliche aber unerwünschterweise gleich benannte Dateien untergehen können und bei der Gutschriften-Erstellung nicht mehr berücksichtigt werden können.

e) Desweiteren ist es möglich, daß Hacker über einen Fremd-PC den Netzbetreiber oder die Evidenz-Zentrale mit unsinnigen Informationen derart "verstopfen", daß die relevanten Übertragungsleitungen für den erwünschten Datenfluß blockiert sind.

Zur Vermeidung dieser Nachteile ist es Aufgabe der Erfindung, ein computerprogrammgesteuertes Verfahren zum gesicherten Aufbau einer Wähl-Leitungsverbindung und zur gesicherten Datenübertragung zwischen einem Chipkarten-Terminal und einer zentralen Datenverarbeitungsanlage unter Ausschluß unbefugten Zugriffes auf diese Leitungsverbindung und/oder die Daten anzugeben, mit anderen Worten, ein Verfahren, welches einen Hackerzugriff äußerst erschwert bzw. unmöglich macht, welches eine sichere Datenübertragung gewährleistet und die Gefahren von Datenverlusten, Falsch- und Doppelbuchungen ausschließt.

Diese Aufgabe der Erfindung wird in vorteilhafterweise durch die im Anspruch 1 angegebenen Merkmale gelöst.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet.

Die Erfindung ist in den Zeichnungen dargestellt und wird im folgenden näher beschrieben. Es zeigen

Fig. 1 ein vereinfachtes Blockschaltbild mit einem Chipkarten-Terminal und zentralen Datenverarbeitungsanlagen für einen bargeldlosen Geldverkehr mit einer Chipkarte zur Anwendung eines bekannten Ver-

BHPA00005702

fahrens nach dem Stand der Technik aber auch zur Anwendung des erfindungsgemäßen Verfahrens,

Fig. 2 eine Wiedergabe einer Übersicht zur Zusammengehörigkeit der Teildarstellungen der Fig. 2A, 2B und 2C,

Fig. 2A, 2B und 2C Teildarstellungen eines schematischen Blockdiagramms zur Verdeutlichung des Ablaufes des erfindungsgemäßen Verfahrens.

Die Fig. 2A, 2B und 2C zeigen zusammengehörend ein schematisches Blockschaltbild des erfindungsgemäßen Verfahrens.

Dieses bezieht sich auf einen gesicherten Aufbau einer Wählleitungsverbindung und eine gesicherte Datenübertragung zwischen einem autorisierten Chipkarten-Terminal 2 und einer autorisierten zentralen Datenverarbeitungsanlage DVA-E 5 bzw. DVA-N 4. Der Block 11 bezieht sich auf die telefonische Anwahl der Datenverarbeitungsanlage 4 oder 5 der Evidenz-Zentrale bzw. des Netzbetreibers. Eine solche Anwahl zielt auf die Herstellung der physikalischen Leitungsverbindung zwischen dem Modem 3 des Chipkarten-Terminals 2 und der empfangenden Datenverarbeitungsanlage 4 bzw. 5 ab. Dabei erfolgt eine Signalisierung (DCD Data Carrier Detect) über eine Steuerleitung.

(Nach dem bekannten Z-Modem-Übertragungsprotokoll offenbart der durch eine telefonische Anwahl adressierte Empfänger seine Bereitschaft zum Empfang einer Datei durch Aussenden eines bestimmten Bereitschaftssignales. Dieses Signal kann eine Einstiegsmöglichkeit für den Hacker in das System bieten). Zur Vermeidung dieser Möglichkeit wird nach Anwahl der Datenverarbeitungsanlage 4 bzw. 5 gemäß dem erfindungsgemäßen Verfahren kein Bereitschaftssignal zum Empfang einer Datei ausgesandt. Die Leitung bleibt logisch tot. Es kommt zum Verbindungsabbruch, sollte auf der Empfangseitung direkt etwas an die Datenverarbeitungsanlage gesendet werden.

Einem Hacker bleibt somit die Empfangsbereitschaft der Datenverarbeitungsanlage verborgen.

Zur Herstellung eines gesicherten Verbindungsaufbaues zwischen Terminal 2 und Datenverarbeitungsanlage 4, 5 dient eine gegenseitige Authentisierung mittels unverschlüsselter und verschlüsselter Zufallszahlen:
Hierzu wird in Block 14 eine 8 Byte umfassende Zufallszahl

A, z. B. 47112345,

erzeugt, in Block 15 zwischengespeichert und in Block 16 an das Terminal 2 gesendet.

Nach Empfang von A wird im Terminal 2 in Block 17 eine Zufallszahl B erzeugt, in Block 18 zwischengespeichert.

In Block 17 wird die empfangene Zufallszahl A zu Av verschlüsselt.

Zur automatischen computerprogrammgesteuerten Verschlüsselung von Information stehen allgemein bekannte elektronische Bauteile mit entsprechenden Verschlüsselungsalgorithmen bereit. Nach Festlegung auf den Verschlüsselungsalgorithmus wird das dafür geeignete elektronische Bauteil an dafür vorhergesehener Stelle des (intelligenten) Terminals und/oder der Datenverarbeitungsanlage eingesetzt. Sobald dieses Verschlüsselungsbauteil programmgesteuert mit einer unverschlüsselten Information beaufschlagt wird, wandelt es diese automatisch entsprechend dem Verschlüsselungsalgorithmus in eine verschlüsselte Information um.

In Block 20 wird durch eine Abfrage sichergestellt, ob das Terminal 2 schon mit einem sogenannten Terminal-Identifikations-Code versehen wurde, durch den das Terminal eineindeutig hinsichtlich Gerätetyp und Konfiguration gekennzeichnet ist. Dieser Code ist an vorgeschriebener Stelle des Terminals gespeichert, er kann programmgesteuert abgefragt werden. Ist ein solcher Terminal-Identifikations-Code vorhanden (in einem solchen Fall ist dieser Terminal-Identifikations-Code auch in der Datenverarbeitungsanlage abgespeichert worden), wird in Block 21 dieser Code TID, zusammen mit der verschlüsselten Zufallszahl Av und der Zufallszahl B als 3 × 8 Byte langer Datensatz an die Datenverarbeitungsanlage 4 bzw. 5 übertragen. Beim Fehlen eines Terminal-Identifikations-Codes TID im Terminal wird zur Kennzeichnung dieses Fehl-Status ein 8 Nullen 0000 0000 umfassender Wert erzeugt (22) und in Block 23 zusammen mit der verschlüsselten Zufallszahl Av und der Zufallszahl B an die Datenverarbeitungsanlage 4 bzw. 5 gesendet.

Beim Vorliegen eines TID wird im Block 21 dieser TID zusammen mit Av und B an die Datenverarbeitungsanlage als 3 × 8 Byte langer Datensatz gesendet.

Zur Vermeidung des Aufwandes, der erforderlich wäre, wenn ein Wartungstechniker beim Fehlen des Terminal-Identifikations-Code am Orte des Terminals erscheinen müßte, um dort in Abstimmung mit der Datenverarbeitungsanlage einen neuen Terminal-Identifikation-Code TIDneu vor zugeben und ihn in das Terminal einzuspeichern, erfolgt erfindungsgemäß die Vergabe und das Einschreiben des TIDneu in das Chipkarten-Terminal automatisch programmgesteuert.

Nach Empfang des im Block 21 bzw. 23 gesendeten 3 × 8 Bytes langen Datensatzes durch die Datenverarbeitungsanlage 4 bzw. 5 wird in Block 24 geprüft, ob zwischen dem Senden der Zufallszahl A in Block 16 und dem Empfang der im 3 × 8 Byte langen Datensatz enthaltenen verschlüsselten Zufallszahl Av durch die Datenverarbeitungsanlage mehr als 3 sec vergangen sind. Diese kurze Zeit bietet eine gewisse Sicherheit, um Hakkern den Einstieg in das System zu verwehren oder zu erschweren, da nicht damit zu rechnen ist, daß ein Hakker in dieser kurzen Zeit den "richtigen" Weg findet.

Sollten mehr als 3 sec vergangen sein, erfolgt Abbruch 25, andernfalls wird das Verfahren fortgeführt wobei in Block 26 die vorgeschriebene Satzlänge geprüft wird. Liegt diese nicht vor, erfolgt Abbruch 25, ansonsten wird der Verfahrensablauf fortgesetzt: in Block 27 wird geprüft wird, ob die in Block 15 zwischengespeicherte Zufallszahl A der im empfangenen Datensatz enthaltenen verschlüsselten Zufallszahl Av entspricht. Nur im Entsprechungsfall wird das Verfahren fortgeführt, ansonsten erfolgt Abbruch in Block 29.

Die Prüfung im Block 27 ist einfach durchzuführen: Die in Block 15 zwischengespeicherte Zufallszahl A wird mit einem wie im Terminal verwendeten Verschlüsselungsbauteil verschlüsselt und das Verschlüsselungsergebnis mit der im 3 × 8 Byte langen Datensatz enthaltenen verschlüsselten Zufallszahl Av verglichen. Bei Gleichheit bestehen keine Bedenken- das Verfahren kann fortgeführt werden.

Es ist aber auch denkbar, daß ein auf das terminalseitig verwendete Verschlüsselungsbauteil abgestimmtes Entschlüsselungsbauteil in der Datenverarbeitungsanlage verwendet wird. Mit diesem würde die im 3 × 8 Byte langen Datensatz enthaltene verschlüsselte Zufallszahl Av decodiert (entschlüsselt) werden; das Entschlüsselungsergebnis müßte bei störungsfreiem Ablauf des Verfahrens mit der in Block 15 zwischengespeicherten Zu-

BHPA00005703

failszahl A übereinstimmen.

Im nachfolgenden Block **28** erfolgt die Abfrage, ob das Kennzeichen 0000 0000 für ein Fehlen des Terminal-Identifikations-Codes vorliegt. Sollte dies der Fall sein, erfolgt in Block **31** die Vergabe eines neuen Terminal-Identifikations-Codes TIDneu aus einem Vorrat zulässiger Werte. Andernfalls wird im Block **30** der im 3 × 8 Byte langen Datensatz enthaltene TID dahingehend überprüft, ob es sich um einen zulässigen Wert handelt, der vormals bei Vergabe dieses Wertes in der Datenverarbeitungsanlage gespeichert wurde. Bei Zulässigkeit wird das Verfahren mit Block **32**, der auch auf Block **31** folgt, fortgesetzt. Im Block **32** wird die vom Terminal mit dem 3 × 8 Byte langen Datensatz empfangene Zufallszahl B zu Bv verschlüsselt (dies erfolgt in Analogie zu der Verschlüsselung der Zufallszahl auf der Terminalseite). Der empfangene zulässige Terminal-Identifikations-Code TID bzw. der neu vergebene Terminal-Identifikations-Code TIDneu werden in Block 32' zwischengespeichert. In Block **33** erfolgt die Übertragung der Werte TIDneu und Bv an das Terminal. Nach Empfang dieser Werte durch das Terminal erfolgt dort im Block **34** die Abfrage, ob nach Absenden der in Block **21** bzw. **23** enthaltenen Information und dem Empfang der im Block **33** enthaltenen Information z. B. mehr als 3 sec. vergangen sind, eine Abfrage, die analog Block **24** zu bewerten ist.

Im Block **36** wird geprüft, ob die in Block **18** zwischengespeicherte Zufallszahl B und die durch Übertragung **33** empfangene verschlüsselte Zufallszahl Bv auch einander entsprechen. Diese Überprüfung erfolgt analog zu der im Block **27** durchgeführten. Nur im Entsprechungsfall wird das Verfahren fortgesetzt. Andernfalls erfolgt Abbruch **35**.

Im Block **37** erfolgt, sofern im Terminal **2** bisher noch kein Terminal-Identifikations-Code eingespeichert war, das Einspeichern des von der Datenverarbeitungsanlage in Block **31** neu vergebenen Terminal-Identifikations-Codes TIDneu. Dieses Einspeichern (hier "Einbrennen" genannt) geschieht programmgesteuert (automatisch). Als Speicher ist ein sogenanntes EEPROM-Element oder ein vergleichbares Bauteil vorgesehen, daß auch spätere Änderungen der eingespeicherten Information zuläßt. Für den Fall, daß das Terminal bereits mit einem Terminal-Identifikations-Code versehen war, wird Block **37** umgangen.

Im Anschluß daran wird in Block **38** unter Bezugnahme auf TID bzw. TIDneu (hierbei handelt es sich um terminalspezifische Daten) eine sogenannte Bezahl-Datei BEZ-Datei erstellt und zwischengespeichert, in der vom Terminal erfaßte Bezahldaten mit chipkarten- und händlerspezifischen Daten zusammengestellt werden. In Block 39 wird diese BEZ-Datei vom Terminal an die Datenverarbeitungsanlage übertragen. Dort wird in Block 40 die empfangene BEZ-Datei zwischengespeichert (vorzugsweise unter einem anderen Datei-Namen, um im Falle der Z-Modem-Besonderheiten ein Überschreiben von Dateien gleichen Namens zu verhindern. Im Block **41** wird geprüft, ob Dateien doppelt angeliefert wurden (eine Doppelverarbeitung identischer Dateien ist zu verhindern, da sie zu unerwünschten Doppelbuchungen führen würde). Hierzu wird die aktuell empfangene BEZ-Datei mit vormals empfangenen und zwischengespeicherten Dateien auf identischen Inhalt überprüft. Im Identitätsfall erfolgt Abbruch **42**, ggfls. mit Fehlermeldung, andernfalls wird die empfangene BEZ-Datei in Block **43** gesichert.

Im Block **44** werden die in der BEZ-Datei enthaltenen Daten zur Bankverbindung des Händlers mit denen in der Datenverarbeitungsanlage gespeicherten Bankdaten des Händlers verglichen. Bei Unstimmigkeiten erfolgt Abbruch **45** (gegebenenfalls wie auch in anderen Abbruchsfällen mit Meldung). Bei Übereinstimmung der Bankverbindungsdaten wird in Block **46** geprüft, ob die in der empfangenen BEZ-Datei enthaltenen TID bzw TIDneu Werte mit den im Block 32' zwischengespeicherten Werten übereinstimmen. Danach kommt es in Block **47** zu einer sogenannten Quittungserstellung, in der die Ergebnisse der Prüfung der BEZ-Datei zusammengestellt sind. Diese Quittung wird in Block **48** an das Terminal **2** gesendet. Dort erfolgt in Block 50 die Verarbeitung der Quittungsinformation. Für den Fall, daß die BEZ-Datei für eine Weiterverarbeitung durch die Datenverarbeitungsanlage im Block 49 akzeptiert werden kann, erfolgt eine Löschung der im Block **38** zwischengespeicherten BEZ-Datei, diese wird nun nicht mehr gebraucht, sie ist ohnehin im Block 43 der Datenverarbeitungsanlage gesichert worden, ihrer Weiterverarbeitung im Block 49 steht nichts mehr entgegen: die Umsatzbeträge können den Händlern auf ihren Computer-Bankkonten gutgeschrieben werden. Sollte sich bei der Überprüfung in Block 51 herausstellen, daß die Quittungsinformation eine Weiterverarbeitung der BEZ-Datei nicht zuläßt, erfolgt Abbruch 52, ggfls mit Fehlermeldung, oder eine Wiederholung bestimmter Vorgänge. Die in Block 46 zwischengespeicherte BEZ-Datei wird deshalb zunächst nicht gelöscht.

Nach dem Löschen der BEZ-Datei in Block 53 beginnt der Verfahrenszyklus wieder mit Block 11. Das erfindungsgemäße Verfahren beinhaltet eine Service-Steigerung für den Kunden: Fehlermeldungen bzw. Abbruchhinweise erfolgen sofort, der Kunde wird zielgerecht geleitet und geführt; es bietet ein hohes Maß an Sicherheit, Komfort, Kundennähe, Datenschutz und Datensicherheit.

Patentansprüche

1. Computerprogrammgesteuertes Verfahren zum gesicherten Aufbau einer Wähl-Leitungsverbindung und zur gesicherten Datenübertragung zwischen einem Chipkarten-Terminal (**2**) und einer zentralen Datenverarbeitungsanlage (**4**, **5**) unter Ausschluß unbefugten Zugriffes auf die Leitungsverbindung und/oder die Daten,
dadurch gekennzeichnet,
a) daß nach Anwahl (**11**) der Datenverarbeitungsanlage durch das Terminal (**2**) von der Datenverarbeitungsanlage (**4**, **5**) ein Zufallswert A generiert (**14**), gespeichert (15) und an das Terminal (**2**) übertragen (**16**) wird,
b) daß vom Terminal (**2**) der empfangenen Zufallswert A zu Av verschlüsselt (**19**), ein Zufallswert B generiert (**17**), gespeichert (**18**) und Av und B an die Datenverarbeitungsanlage übertragen (**21**, **23**) werden,
c) daß von der Datenverarbeitungsanlage (**4**, **5**) geprüft: (**27**) wird, ob A und Av einander entsprechen und daß im Entsprechungsfall von der Datenverarbeitungsanlage (**4**, **5**) der empfangene Zufallswert B zu Bv verschlüsselt (**32**) und an das Terminal (**2**) übertragen (**33**) wird,
d) daß vom Terminal (**2**) geprüft (**36**) wird, ob B und Bv einander entsprechen,
e) daß ein im Terminal (**2**) gespeicherter Terminal-Identifikations-Code TID bzw. ein Si-

BHPA00005704

gnal F für ein Fehlen dieses Codes vom Terminal (2) an die Datenverarbeitungsanlage (4, 5) übertragen (21, 23) wird,

f) daß von der Datenverarbeitungsanlage (4, 5) beim Empfang des Terminal-Identifikations-Codes TID durch Vergleich (30) desselben mit allen gültigen in der Datenverarbeitungsanlage (4, 5) gespeicherten Terminal-Identifikations-Codes geprüft wird, ob der empfangene Terminal-Identifikations-Code TID zulässig ist bzw. daß von der Datenverarbeitungsanlage (4, 5) beim Empfang des Signales F ein neuer Terminal-Identifikations-Code TIDneu generiert (31) wird und

g) daß dieser (TIDneu) an das Terminal (2) gesendet (33) und dort zu dessen (2) künftiger Kennzeichnung eingespeichert (37) wird,

h) daß der — gemäß e) — von der Datenverarbeitungsanlage (4, 5) empfangene Terminal-Identifikations-Code TID bzw. — der gemäß f — generierte neue Terminal-Identifikations-Code TIDneu für eine spätere Prüfoperation in der Datenverarbeitungsanlage (4, 5) zwischengespeichert (32') wird,

i) daß im Entsprechungsfall — gemäß d) — B entspricht Bv und bei Vorliegen eines Terminal-Identifikations-Codes TID bzw. eines neuen Terminal-Identifikations-Codes TIDneu im Terminal (2) eine dort (2) zwischenzuspeichernde Zahlbeträge, terminal-, chipkarten- und terminalbesitzer-spezifische Daten umfassende Datei erstellt (38) und an die Datenverarbeitungsanlage (4, 5) übertragen (39) wird,

j) daß diese Datei von der Datenverarbeitungsanlage zwischengespeichert (40) und mit vorhergehenden empfangenen Dateien auf Identität ihres Inhaltes zum Ausschluß von Datei-Doppelverarbeitungen verglichen (41) wird,

k) daß die — gemäß h — in der Datenverarbeitungsanlage (4, 5) zwischengespeicherten Werte (32') TID bzw. TIDneu mit denen in der von der Datenverarbeitungsanlage (4, 5) empfangenen Datei enthaltenen Werten TID bzw. TIDneu auf Übereinstimmung geprüft (46) werden,

l) daß von der Datenverarbeitungsanlage (4, 5) nach erfolgter Dateiprüfung eine die Prüfergebnisse enthaltende Quittierungsinformation erstellt (47) und an das Terminal (2) übertragen (48) wird, und

m) daß im Terminal (2) nach Vorliegen einer für die Weiterverarbeitung (49) der Datei zu akzeptierende Quittierungsinformation die — gemäß i — zwischengespeicherte Datei gelöscht wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß nach Ablauf einer vorgegeben Zeit (im einstelligen Sekundenbereich), gerechnet ab Übertragungsbeginn (16) des Zufallwertes A bis zum Empfang des verschlüsselten Zufallswertes Av durch die Datenverarbeitungsanlage die Leitungsverbindung abgebrochen (25) wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß nach Ablauf einer vorgegeben Zeit (im einstelligen Sekundenbereich), gerechnet ab Übertragungsbeginn (21) des Zufallwertes B bis zum Empfang des verschlüsselten Zufallswertes Bv durch das Terminal (2) die Leitungsverbindung abgebrochen (35) wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß nach der Anwahl (11) der Datenverarbeitungsanlage (4, 5) die Leitungsverbindung abgebrochen (13) wird, wenn als erstes auf der Anwählleitung Daten an die Datenverarbeitungsanlage gesendet werden.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Terminal-Identifikations-Code TID bzw. das Signal F — gemäß e) —, der — gemäß b) — verschlüsselte Zufallswert Av und der Zufallswert B — gemäß b) — in einem Übertragungsschritt als Datensatz definierter Satzlänge vom Chipkarten-Terminal (2) an die Datenverarbeitungsanlage (4, 5) übertragen (21, 23) werden, und daß beim Empfang dieses Datensatzes von der Datenverarbeitungsanlage (4, 5) dessen vorgeschriebene Satzlänge geprüft (26) wird.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zum Ausschluß (41) von Doppelverarbeitungen von Dateien, die aktuelle von der Datenverarbeitungsanlage (4, 5) empfangene Datei unter einem anderen Dateinamen zwischengespeichert wird, wobei sich die Identitätsprüfung auf den Dateiinhalt bezieht.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei der Dateiprüfung die in der Datei enthaltenen terminalbesitzer-spezifischen Bankverbindungsdaten mit den in der Datenverarbeitungsanlage gespeicherten Bankverbindungsdaten aller Terminalbesitzer verglichen (44) werden.

Hierzu 5 Seite(n) Zeichnungen

BHPA00005705

– Leerseite –

BHPA00005706

Nummer: DE 196 41 776 A1
Int. Cl.[6]: H 04 L 12/22
Offenlegungstag: 13. März 1997

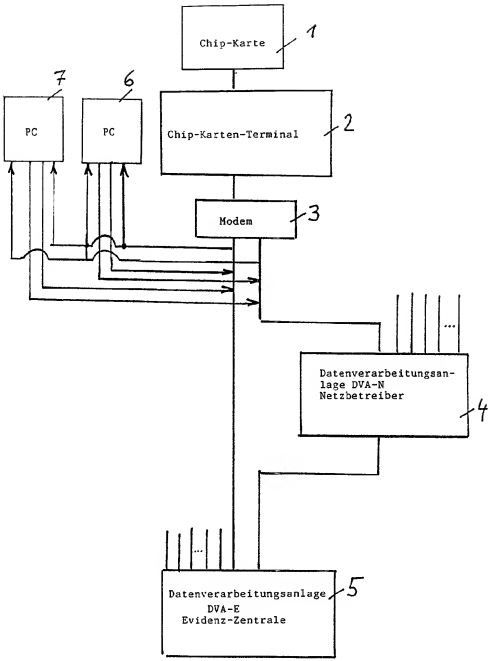


FIG. 1

602 071/614

BHPA00005707

Nummer: DE 196 41 776 A1
Int. Cl.[6]: H 04 L 12/22
Offenlegungstag: 13. März 1997

FIG. 2

BHPA00005708

Nummer: DE 196 41 776 A1
Int. Cl.⁶: H 04 L 12/22
Offenlegungstag: 13. März 1997

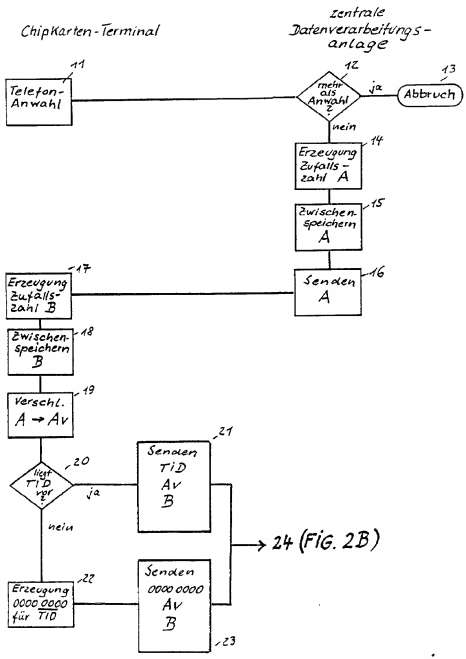


FIG. 2A

602 071/614

BHPA00005709

Nummer: DE 196 41 776 A1
Int. Cl.[6]: H 04 L 12/22
Offenlegungstag: 13. März 1997

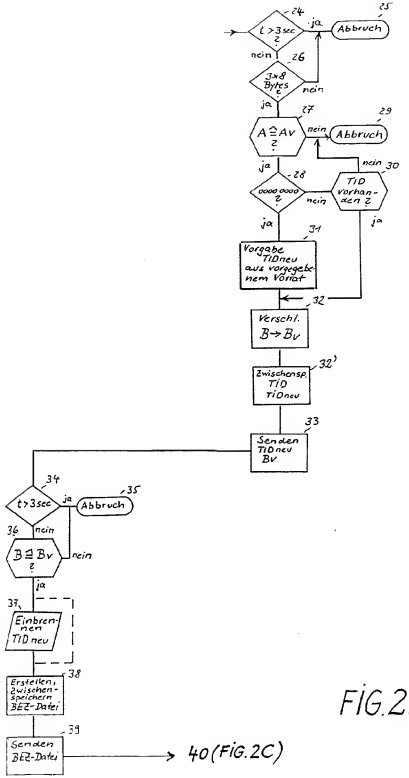


FIG. 2B

602 071/614

BHPA00005710

Nummer: DE 196 41 776 A1
Int. Cl.[6]: H 04 L 12/22
Offenlegungstag: 13. März 1997

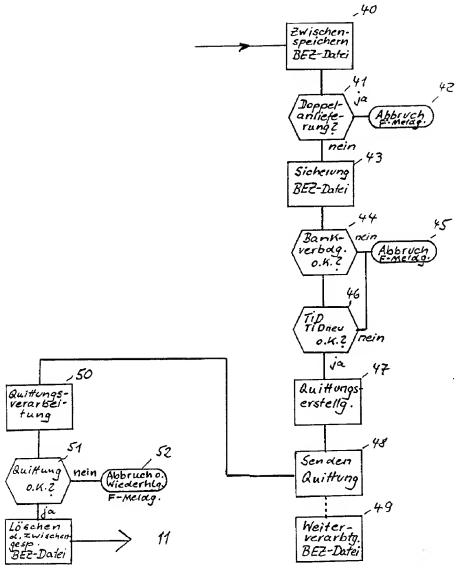


FIG.2C

602 071/614

BHPA00005711